TACTICAL WEAPON
GACIAC
GUIDANCE & CONTROL
INFORMATION ANALYSIS CENTER

GACIAC SR-84-01

DOMESTIC TECHNOLOGY TRANSFER VERSUS TECHNOLOGY EXPORT CONTROL —

THE EMERGING NATIONAL POLICIES AND THE ROLE OF THE BENCH ENGINEER

January 1984

Howard C. Race
Technology Transfer Staff-Specialist
US Army Missile Command

Published by GACIAC
IIT Research Institute
10 West 35th Street
Chicago, Illinois 60616

DoD Technical Sponsor:
Joint Service Guidance and Control Committee
Members from OUSDR&E, Army,
Navy, Air Force, and DARPA

NOTICES

Special Report. This Report has been published by the Tactical Weapon Guidance and Control Information Analysis Center (GACIAC) as a service to the defense community. GACIAC is a DOD Information Analysis Center, administered by the Defense Technical Information Center, operated by IIT Research Institute under Contract No. DLA900-80-C-2853. GACIAC is funded by DTIC, DARPA, and US Army, US Navy, and US Air Force Laboratories/Controlling Activities having an interest in tactical weapon guidance and control. The Contracting Officer is Mrs. S. Williams, DESC, Dayton, Ohio. The Contracting Officer's Technical Representative and author of this report is Mr. H. C. Race, US Army Missile Command, ATTN: DRSMI-RN, Redstone Arsenal, Alabama 35898.

Comments, Criticisms, and Corrections. Please send comments to: Commander, US Army Missile Command, ATTN: DRSMI-RN (H. Race), Redstone Arsenal, Alabama 35898. Telephone: (205) 876-4406; Autovon 746-5449.

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER: GACIAC SR-84-01	2. GOVT ACCESSION NO.
3. RECIPIENT'S CATALOG NUMBER	
4. TITLE (and Subtitle): Domestic Technology Transfer Versus Technology Export Control - The Emerging National Policies and the Role of the Bench Engineer	5. TYPE OF REPORT & PERIOD COVERED: Special Report
	6. PERFORMING ORG. REPORT NUMBER: GACIAC SR-84-01
7. AUTHOR(s): Howard C. Race	8. CONTRACT OR GRANT NUMBER(s): DLA900-80-C-2853
9. PERFORMING ORGANIZATION NAME AND ADDRESS: GACIAC/ITT Research Institute, 10 West 35th Street, Chicago, Illinois 60616	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS	12. REPORT DATE: January 1984
	13. NUMBER OF PAGES: 73
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)	15. SECURITY CLASS. (of this report): UNCLASSIFIED
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

This special report is only available from GACIAC. Reproduction is not authorized except by specific permission.

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Technology Transfer
Export Control
Munitions Control
Information Security
Technical Information
Militarily Critical Technology

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

Domestic technology transfer is the positive exchange of information among the members of the scientific and engineering communities within the US, both defense and non-defense related. Technology export can be intentional or non-intentional, and the results can produce strategic benefits/detriments to the nation's economic, political, and military goals. The dichotomy and the dynamics of the national policies and directives on these two aspects of technology transfer are discussed for the bench engineer. The roles of the bench engineer in the government laboratory, industrial R&D center, and the

university research facility/laboratory, are delineated. Guidance is provided on how to separate classified information from unclassified militarily significant technology, and from other unclassified technology information. The active participant role for the bench engineer is advocated to accomplish national security objectives through encouraging domestic technology transfer and preparing accurate technology assessments for considerations in export control case processing.

JANUARY 1984 GACIAC SR-84-01

DOMESTIC TECHNOLOGY TRANSFER VERSUS TECHNOLOGY EXPORT CONTROL —

THE EMERGING NATIONAL POLICIES AND THE ROLE OF THE BENCH ENGINEER

HOWARD C. RACE
DEPARTMENT OF THE ARMY

Published by GACIAC
IIT Research Institute
10 West 35th Street
Chicago, Illinois 60616

GACIAC - - A DoD Information Analysis Center
Operated by IIT Research Institute, 10 W. 35th St., Chicago, IL 60616
DoD Technical Sponsor - Joint Service Guidance and Control Committee
Members from OUSDR&E, Army, Navy, Air Force, and DARPA

ACKNOWLEDGEMENTS

The author is grateful for the technical, administrative, editorial, and consultative guidance and support provided by the following Defense community personnel:

Ms. Carol Burch, MICOM

Mr. Jack Kolb, DARCOM

Ms. Janice Lee, MICOM

Dr. William Leonard, MICOM

Dr. Oles Lomacky, OUSDRE, IP&T

Mr. Nick Mangus, MICOM

Ms. Ellen McCauley, DTIC

Mr. Jacques Naviaux, Hughes Aircraft Co.

Mr. Jim Pendergast, DTIC

Ms. Edna Prichard, MICOM

Mr. Chuck Smoots, IITRI/GACIAC

Mr. Frank Sobieszczyk, OUSDRE (R&AT)

Mr. Waite Todd, Chairman JSGCC

Ms. LaDoris Wiley, MICOM

Ms. Linda Yancey, MICOM

TABLE OF CONTENTS

LIST OF TABLES

Domestic Technology Transfer Versus Technology Export Control - The Emerging National Policies and The Role of the Bench Engineer

I. Introduction

A. The Three Faces of Technology Transfer

Technology transfer means different things to many people. Sometimes technology transfer means the rational progressive movement or hand-off of technology from basic research (6.1) to exploratory development (6.2), to advanced development (6.3a and b), to engineering development (6.4), and to the acquisition, fielding and life cycle support of military equipment. "Technology infusion" is also an integral part of logistics R&D, integrated logistics support, manufacturing methods and technology, and pre-planned product improvements.

Secondly, technology transfer has been understood to be the positive exchange of scientific, technical, engineering, and manufacturing data and know-how among and within academia, industry, and Government agencies to the enhancement and growth in the overall body of knowledge. Benefits are accrued by harnessing the laws of

physics and science for mankind. Economic benefits are obtained by competitive industry in the marketing of new and innovative products that push the state-of-the-art. Increased sophistication in technology also allows the military-industrial complex to develop new and improved capability weapons and equipment to support the nation's fighting forces.

Thirdly, technology transfer has become the dominant phrase when concerned with the loss of technology across our borders which may result in a detrimental impact to our national defense posture and cause reductions in our industries' economic well being.

This report is intended to clarify for the bench engineer and others the differences in the last two faces of technology transfer so that the first face (rational movement) can be pursued. The bench engineer and his supervisor, whether employees of a Government laboratory, a defense contractor, or a university/college research facility, need to understand the dichotomy of views surrounding the evolution of the nation's policies in "domestic technology transfer" and "technology export control." The bench engineer must become the "subject matter expert" (world-wide authority) so that the correct technical assessments and recommendations can be provided to the captains of industry and the elected and appointed officials of the Government to effect national policy decisions. The engineer's factual technical recommendations can then be balanced against economic, political, and military considerations.

B. The Dichotomy

Technology advancements are known to produce an increase in a nation's economic prosperity, while at the same time improving its military preparedness either directly or indirectly. Obviously the United States wants to maximize domestic technology transfer and manage or control the export of all technology to our Allies and friendly non-aligned nations, to assure our favorable economic position in the world market, and/or enhance our Allies' military stature for the overall benefit of the free world. Likewise, we want to minimize technology export to our potential adversaries to maintain, gain, or regain economic and/or military advantages. Unless, of course, there is a political decision that would have us make a purposeful technology export for a particular reason. It must be kept in mind that the US may not be the world leader in all fields of science and engineering and that intentional technology export could yield a beneficial reciprocal technology import.

The technology transfer controversy arises over Government control of military hardware/software and technical data related to science, technology, research, development, manufacturing, test, operation, and maintenance of weapons/munitions and military equipment. For obvious national security reasons some of this information is classified, and some is not. Some of the generally unclassified information has been labeled as "militarily critical technology" and subject to export control laws. Clouding the issue is the fact that some

technology has a "dual-use" (both military and non-military application), and that means the "end-use" abroad may be in question. One of the most prominent questions surrounds the position that governmental control of basic research technologies is contrary to the established "openness" atmosphere in the United States academic arena. Similarly, US industry is concerned about corporate profits that may be maximized in the world market place by the sale of their goods and services -- both military and commerical. Industry is frequently perturbed by excessive delays and inconsistencies in processing munitions control cases and the voluminosity of the Militarily Critical Technologies List (MCTL).

The bench engineer is frequently called upon to express his expert technical opinion on the status of a technology development, the classification of technical data or information, and/or the military significance of the technology. In order for him to perform this job more effectively, he needs to understand the breadth and depth of domestic technology transfer, how it is structured, and the role that he plays in it. Likewise, an appreciation of the national disclosure policies, their evolution and direction, will be helpful in assisting the bench engineer in ascertaining and improving his role in the nation's technology growth and national defense.

C. The Holes in the Dike

The body of US scientific and technical knowledge is analogous to the water in a reservoir. The US is continually trying to build up its capacity through positive contributions while limiting the uncontrolled discharge and leaks. Our open society affords friends and foes alike the opportunities to obtain scientific knowledge just for the asking, for a fair price, and by less than honorable means. Specifically why do potential adversaries want our technology? How do they obtain it? And what target technologies are they after?

Why acquire Western technology?

> The Soviets and their Warsaw Pact Allies have derived significant military gains from their acquisitions of Western technology, particularly in the strategic, aircraft, naval, tactical, microelectronics, and computer areas. This multifaceted Soviet acquisitions program has allowed the Soviets to:
>
> - Save hundreds of millions of dollars in R&D costs, and years in R&D development leadtime...
> - Modernize critical sectors of their military industry and reduce engineering risks by following or copying proven Western designs, thereby limiting the rise in their military production costs.
> - Achieve greater weapons performance than if they had to rely solely on their own technology.
> - Incorporate countermeasures to Western weapons early in the development of their own weapon programs.
>
> These gains are evident in all areas of military weapons systems.[1]

How is technology transferred? The Bucy Report succinctly states:

> The many mechanisms for transferring technology may be arranged in a spectrum stretching from the most active where the donor actively transfers design and manufacturing know-how; e.g. establishing a "turn-key" factory, to the most passive where the donor is passive in regard to know-how transfer; e.g., a trade exhibit.
>
> "Active" relationships involve frequent and specific communications between donor and receiver. These usually transfer proprietary or restricted information. They are directed toward a specific goal of improving the technical capability of the receiving nation. Typically, this is an interactive process: the receiver requests specific information, applies it, develops new findings, and then requests further information. This process is normally continued for several years, until the receiver demonstrates the desired capability.
>
> "Passive" relationships, from a technology transfer viewpoint, imply the transfer of information or products that the donor has already made widely available to the public. Passive mechanisms do little to transfer technology.[2]

Potential technology transfer channels can be categorized as overt (lawful, political, economic) or covert (less than honorable). The quality and quantity of the technology transferred (exported) can vary tremendously as can the level of public knowledge (the cognizance of the victim) [See Table 1].

Table 1. Potential Technology Transfer Channels[3]

OVERT

Method	Active/Passive
1. Legal Direct Equipment Purchases	A
2. Legal Third-Country Purchases	A
3. Equipment Captured in Wars	A
4. Legal Licenses and Patents	A
5. Turn-Key Plant Sales	A
6. Joint Ventures	A
7. Direct Commercial Know-How	A
8. Trade Shows, Exhibits, Conferences	P
9. Academic Exchanges	P
10. Open Literature, Including Government Publications	P
11. Deliberate US Government Leaks	P

COVERT

1. Illegal Direct Equipment Purchases	A
2. Illegal Third-Country Diversions	A
3. Bribes to Western Nationals	A
4. Third-Country Visitors to United States	A
5. Industrial Espionage	A
6. Foreign Agents	A

Now that we know why our adversaries want Western technology and how they go about getting it, let's see what they are after. In the unclassified CIA report, "Soviet Acquisition of Western Technology," which is favorably accepted throughout the executive and legislative branches of the US Government, certain technologies and equipments are identified as projected Soviet technological needs and acquisition targets through the 1980's. They range from manufacturing and programming information for computers to propulsion systems technology and sensor systems technology [See Table 2]. Are you working in one or more of these technology areas?

How do we plug the holes and continue to fill the reservoir? Let's examine how domestic technology transfer takes place, the norms, the applicable laws of the land, and how the bench engineer participates in the system. Then we need to review the National Security Information Program to see how and why some information is classified and to what degree. Next we shall study the evolution and present status of controls for <u>intentional</u> technology export and controls to limit <u>undesirable</u> technology export. In summary we will list the do's and don'ts for the bench engineer that will ensure his active and authoritative participation as a technical "subject matter expert."

In conclusion, we will establish a perspective on the role of the bench engineer and his supervisor on domestic technology transfer and technology export control.

Table 2. Projected Soviet Technological Needs and Acquisition Targets through the 1980's.[4]

1. Microelectronics and computer technology for in-flight guidance computers.

2. Latest generation of US inertial components upon which the MX ICBM and the TRIDENT SLBM guidance systems are based.

3. Solid rocket propulsion design and production technology.

4. Anti-Ballistic Missile (ABM) technology.

5. Composite aircraft materials technology.

6. High-bypass turbofan for large strategic airlift type of aircraft.

7. Accurate airborne inertial navigation systems for long-range navigation and weapons delivery.

8. Computer-aided aircraft design technology.

9. Aircraft production technology.

10. Advanced signal processing for air defense radars and missiles.

11. Acoustic sensor technology.

12. Submarine quieting technology.

13. Precision submarine inertial navigation systems.

14. Large aircraft carrier design and construction technologies.

15. Electrooptical antitank seeker and sensor technology for tactical missiles.

16. Signal processing and microelectronics technologies supporting tactical weapon systems.

17. High-volume production technology for large-scale integration (LSI) circuits.

18. Microelectronic materials for integrated-circuit production.

19. Technologies for very high-speed integrated circuit (VHSIC).

20. "Superminicomputer" technology.

21. Network-control software programs related to networking.

II. Domestic Technology Transfer

A. Non-Defense Technology Transfer Fundamentals

The nation's technological reservoir is filled by the basic scientific research conducted in our 150 research universities throughout the states.[5] While the universities are basically educational institutions, they have taken on the role of research centers as an inseparable responsibility and necessity. The senior scientist professor and his graduate student apprentice frequently make orginal contributions to the research frontier. Today, the universities conduct more than one-half of the basic research in the country with only about 10% of the total R&D dollar.[6] This body of knowledge is communicated in many different ways. Our scientists publish their findings in many of the over 2000 international technical journals.[7] They attend scientific meetings and symposiums to present their findings and listen to their colleagues. They conduct daily and weekly less formal technical discussions with their fellow scientists, graduate students and other interested researchers both in the US and abroad.

These technical discourses on principally non-defense related subjects are, in many instances, transferred to industrial R&D centers and commercial engineering laboratories to become "productized" for consumer goods. Sometimes technological design and know-how is stamped "proprietary" by its owner and safeguarded with every facility available except maybe an armed guard. This proprietary information and its benefits

are held for timely disclosure to maximize sales potential and thus optimize corporate profits. The "bad guys" are the competition - both foreign and domestic. The market of today and the future belongs to the successful "secret keeper," with the right technical solution.

B. Governmental Stimuli to Technology Transfer

From the defense/industry/academia science and technology perspective, basic and applied research is performed in government laboratories and conducted for the government by defense contractors and university research facilities/laboratories. Typical Department of Defense contracting agencies for research include the Army, Navy, and Air Force Laboratories, Army Research Office, Office of Naval Research, Air Force Office of Scientific Research, and the Defense Advanced Research Projects Agency (DARPA).

Contracted work can either be classified or unclassified. Unclassified work can be identified as militarily critical or otherwise. (Both of these ramifications will be explored in detail later in this report.) Most major defense contractors have their own additional "Independent Research and Development" (IR&D) program to produce technology expertise increases to improve their competitive edge. The government allows the defense contractor to recoup most of his investment through future "general and administrative" (G&A) overhead rates against direct costs. Percentages are based on the government's evaluation of the contractor's entire IR&D program brochure on relevance and productivity.

Academic research facilities perform a wide variety of basic research and exploratory development tasks for government and industrial defense contractors. This work may also be classified or unclassified.

The exchange of defense produced technology takes place through official Government publications, closed Government/contractor conferences or workshops, and restricted access symposiums sometimes co-sponsored by non-government organizations such as the Association of the United States Army (AUSA), the American Defense Preparedness Association (ADPA), and the Air Force Association (AFA), which support national defense objectives. Other written and verbal information about defense produced technologies is also transferred through scientific journals, open meetings, and symposiums just as for the non-defense technologies generated outside the Government. It is the law of the land and the Department of Defense (DoD) policy to provide the American people with the maximum information about DoD operations and activities. To this end there are many established Federal programs to effect dissemination of information among Government agencies and to the American public for the expressed purpose of enhancing our "technology quotient" and our military/economic well being.

1. Information Programs

The regulations governing the exchange of Defense Scientific and Technical Information (STI) are established by DoD Directive 3200.12, "DoD Scientific and Technical Information Program" (STIP). Execution is accomplished by every technology producing DoD agency and by the Defense Logistics Agency (DLA) through its Defense Technical Information Center (DTIC) which is located at Cameron Station in Alexandria, Virginia. When a technical report is prepared by a DoD agency or defense contractor, it is given primary dissemination directly to other defense agencies and specific industrial/academic facilities known to be participating in the development of that specific defense related technology. Most documents are also placed in the repository of DTIC where their abstracts, titles, etc., are announced biweekly in the "Technical Abstract Bulletin (TAB)" to alert registered Government agencies and defense contractors of their existence and availability for secondary distribution. The TAB and its annual index are classified confidential. Authorized Government agencies can request copies of available reports directly from DTIC. To obtain "limited distribution" reports, defense contractors in the past initiated a request that required the concurrence of their sponsoring contracting officers' technical representative (COTR) (Government bench engineer) and approval of the report's originating agency. Two new distribution limitation statements (discussed later in detail in Chapter III) will provide for rapid access by certified Government agency contractors and/or DoD contractors who have a generalized "need-to-know." Classified reports can be obtained by

defense contractors provided they are registered as a cleared and approved organization on the Dissemination Authority List (DAL) to receive information in particular subject fields (certified by a Defense Department sponsor).

The DoD Instruction 5200.21, "Dissemination of DoD Technical Information," assigns responsibilities for the dissemination of DoD technical information and establishes certification procedures for access to that information. Defense contractors initiate DD Form 1540, "Registration for Scientific and Technical Information Services," and obtain approval from their sponsoring agency's COTR for specific subject fields. Prospective defense contractors registered in the Army's Qualitative Requirements Information (QRI) program or "Potential Contractor Program" can obtain sponsorship by an Army agency's Technical Industrial Liaison Officer (TILO) and thus gain access to relevant unclassified technical information for future solicitations and proposals. All qualified DTIC users are listed in the "Dissemination Authority List" published quarterly by DTIC. The bench engineer (report author) is generally knowledgeable as to who throughout Government and industry is already interested in and participating in developing his specific technology. The bench engineer in Government or industry working through his local supporting technical library, such as the Redstone Scientific and Technical Information Center (RSIC), obtains subject matter bibliographic search synopses and selected reports to support his projects.

2. Information Analysis Centers

To facilitate the acquisition and analysis of specific technical information in a narrow field, the Department of Defense has established 19 Information Analysis Centers (IAC'S). Some centers are organized along the discipline line, i.e: plastics, or metals; other centers have a mission area orientation, i.e: guidance and control, or infrared technology [See Table 3]. Of these 19 IAC'S, 9 are administered and partially funded by the DTIC. The other IAC's are specific service funded and managed. Each center receives management from a DoD laboratory or agency that has competence in the field of science and technology for which that particular center functions. In addition, technical expertise is provided by practicing scientists and engineers associated with the research and development facility.

As all source collection centers for a particular technical field, each IAC receives technical documention input via primary distribution from all pertinent DoD agencies and their contractors as authorized by the Contracting Officer's Technical Representative (COTR). Likewise, the IAC's support DoD agencies, DoD contractors, other Government agencies and their contractors, and university research facilities/laboratories provided they are eligible users. The Information Analysis Centers generally offer the categories of products/services shown in Table 4.

Table 3. Information Analysis Centers[8]

Title	Location	DTIC Administration	Technical Management
Coastal Engineering Information Analysis Center (CEIAC)	US Army Engineer Waterways Experiment Station	No	Army
Chemical Propulsion Information Agency (CPIA)	Applied Physics Laboratory John Hopkins University	Yes	Navy, NAVSEA
Cold Regions Science and Technology Information Analysis Center (CRSTIAC)	Cold Regions Research and Engineering Lab	No	Army
Concrete Technology Information Analysis Center (CTIAC)	US Army Engineer Waterways Experiment Station	No	Army
Data and Analysis Center for Software (DACS)	Rome Air Development Center	Yes	RADC Air Force
DoD Nuclear Information and Analysis Center (DASIAC)	Kaman-TEMPO Santa Barbara, CA	No	Defense Nuclear Agency
Guidance and Control IAC (GACIAC)	IIT Research Institute Chicago, IL	Yes	Army, MICOM
Hydraulic Engineering IAC (HEIAC)	US Army Engineer Waterways Experiment Station	No	Army
Infrared Information and Analysis Center (IRIA)	Environmental Research Institute of Michigan	Yes	Navy, ONR

Table 3. Information Analysis Centers (Cont'd)

Title	Location	DTIC Administration	Technical Management
Metals and Ceramics Information Center (MCIC)	Battelle-Columbus Laboratories	Yes	OUSDRE (R&AT)
Metal Matrix Composites IAC (MMCIAC)	Kaman-TEMPO Santa Barbara, CA	Yes	OUSDRE (R&AT)
Nondestructive Testing IAC (NTIAC)	Southwest Research Institute San Antonio, TX	Yes	OUSDRE (R&AT)
Plastics Technical Evaluation Center (PLASTEC)	Armament R&D Center	No	Army, ARDC
Pavements and Soil Trafficability Information Analysis Center (PSTIAC)	U.S. Army Engineer Waterways Experiment Station	No	Army
Reliability Analysis Center (RAC)	Rome Air Development Center	Yes	Air Force, RADC
Soil Mechanics Information Analysis Center (SMIAC)	U.S. Army Engineer Waterways Experiment Station	No	Army
Shock and Vibration Information Center (SVIC)	Shock and Vibration Information Center, Naval Research Lab	No	Navy, NAVSEA
Tactical Technology Center (TACTEC)	Battelle-Columbus Laboratories	No	DARPA
Thermophysical and Electronic Properties Information Analysis	CINDAS, Purdue University	Yes	OUSDRE (R&AT)

Table 4. Products and Services of Information Analysis Center[9]

Abstracts and Indexes - Announcements in the form of abstracts and indices of pertinent reports in the IAC's field of interest.

Technical Inquiry Services - Authoritative advice in response to technical questions posed by the user.

Bibliographic Inquiry Service - References to the latest and most relevant authoritative reports covering user's inquiry.

Scientific and Engineering Reference Works - Useful and authoritative information applicable to on-going work through design, preparation and maintenance of handbooks and data books.

State-of-the-Art Reports - Summaries of the status of technologies that are pertinent to current research, development, test and evaluation (RDT&E) decision making with usefulness extending from the bench level to all levels of RDT&E management.

Critical Reviews and Technology Assessments - The latest scientific or engineering information in the most useful format on subjects of significant interest to the Defense RDT&E community. Those reviews and assessments may provide comparative analyses of technologies based on technical, national and/or geographic considerations.

Current Awareness - Newsletters and reviews to keep the Centers' users appraised of the latest and most significant technological development within the Center's field of interest.

Special Studies/Tasks - Detailed problem solution information which is narrow in scope.

Technical Conference/Interagency Committee Organization and Administration - Adminstrative and technical support to technical conferences and joint committees in the Department of Defense. The purpose of these committees is to solve problems, effect coordination of technology programs, and promote an exchange of technical information.

It should be noted that the IAC's do not make secondary distribution of technical documents provided to them by other agencies/ contractors. Primary distribution of each IAC's self-generated documents (products) is made to interested and qualified recipients.

Funding for the basic operation of the DTIC administered IAC's is provided by DLA/DTIC. Generalized support to DoD committees/working groups and short term investigations for government engineers are obtained as a result of block funding from the "services" which are regularly supported. Specific longer term (4 days to 6 months) investigative tasks are funded by the Government and industry requiring organizations. All Government agencies are provided products and services by virtue of the "services" block funding. Many defense contractors and university research centers are "paying subscribers" for the IAC's products and services. Other non-subscribers purchase products and services from the IAC's on an "as-needed/identified" basis. The IAC's technical information operations are on a cost reimbursable system.

3. Public Technical Information

Complementing the "DoD Community" Scientific and Technical Information Program is the Department of Commerce's National Technical Information Service (NTIS). The NTIS, located in Springfield, Virginia, receives all DoD technical publications that have been "approved for public release - distribution unlimited" and other US Government produced research, development and engineering reports. The NTIS has over 1 Million titles of which about 300,000 cite foreign technology.[10] Access to bibliographic abstracts is obtained through on-line computer data bases, and printed biweekly and annual indices. Annually, more than 6 million reports are provided world-wide for a nominal cost to cover operations and distribution expenses. Obviously this is an excellent domestic technology transfer mechanism for all Government agencies, American industry, university requirements and any American citizen. Of concern though, is the fact that while information in NTIS has been determined suitable for public release, the availability of this "cheap to obtain" technology can provide our friends and Allies economic advantages and can provide our potential adversaries an economic boost resulting indirectly in enhanced military capability. Even though this may be the case, Congress has established an "openness" policy on transfer of federally funded technology to state and local governments and to the private sector. It is interesting to note that until recently the Soviet Embassy in Washington, DC, had a standing order for two copies of every report available from NTIS.

4. Technology Innovation Act

In the Stevenson-Wydler Technology Innovation Act of 1980, the Congress mandated that all federally funded laboratories establish an Office of Research and Technology Applications (ORTA) "to provide and disseminate information on federally owned or originated products, processes, and services having a potential application to state and local government and to private industry." The act also required that the Department of Commerce establish a Center for the Utilization of Federal Technology (CUFT). The CUFT was institutionalized as a part of the NTIS. The dissemination process is initiated by the federally funded bench engineer who identifies that serendipitous utilization of his technology may be a solution to some problem in the state, local or private sector. A brief "technology application assessment" is prepared by the bench engineer and his laboratory ORTA officer and then provided through channels to the CUFT via the secretariat of the Federal Laboratory Consortium (FLC) for technology transfer.

The FLC is an organization made up of more than 350 Federal laboratories and centers from 11 Federal agencies. The FLC coordination function is performed on a voluntary (additional duty basis) by six regional and four national technology transfer specialists from throughout the Federal laboratory system and their contractors. The technology developed through the efforts of the Federal Government is a national resource. This resource is particularly valuable in the development of new products or processes

for use by both the public and private sectors. Gaining access to this resource can be a complicated task because of the many agencies and individual laboratories involved. The FLC was conceived and designed to improve the accessibility of this resource for state and local governments as well as domestic industries. The FLC establishes person-to-person contacts between the Federal laboratories and potential public and private sector users. The FLC and CUFT at NTIS complement each other in ensuring that execution of the Technology Innovation Act is effective.

The domestic technology transfer arena is rounded out by a dozen professional and commercial organizations that promote the accomplishment of technology transfer. Of noteworthy mention is the "Technology Transfer Society" (T^2S) which held its Eighth Annual Meeting and International Symposium in June 1983 on the subject: "Pecple Interaction - The Key to Technology Transfer."

5. The Freedom of Information Act

The Freedom of Information Act (FOIA) (Title 5, US Code, Section 552) postulates that openness in Government is good, and that the American public has a right to know almost everything that the Government is doing. Those "other things" are of course known by elected and appointed officials who cause them to happen. Certain "checks and balances" within our three part Government ensure adherence to the United States Constitution. The act provides that nine categories of information or records may be withheld from public disclosure unless otherwise prescribed by law. Generally those exemption categories are:

a. Information properly classified under criteria established by Executive Order.

b. Information or regulatory issuances relating to internal personnel rules or practices.

c. Matters that another statute specifically exempts from disclosure.

d. Trade secrets or commercial or financial information received in confidence from outside the government.

e. Internal advice, recommendations, and subjective evaluations pertaining to the decision-making process.

f. Information in personnel or medical files.

g. Investigative records compiled for enforcing civil, criminal, or military law.

h. Information contained in or related to examination, operation or condition reports used by agencies responsible for the regulation or supervision of financial institutions.

i. Certain geological and geophysical information and data concerning wells.

Department of Defense Directive 5400.7, "DoD Freedom of Information Act Program," contains two policy statements relevant to technology transfer:

> a. "Promote public trust by making the maximum amount of information available to the public on the operation and activities of the Department of Defense, consistent with DOD's responsibility to ensure national security"; and
>
> b. "Release records to the public, unless those records are exempt from mandatory disclosure as outlined in chapter III of DOD 5400.7-R."[11]

The DoD policy obviously promotes domestic technology transfer by "maximizing" the amount of information available to the public, but, on the other hand, it has compounded the technology export "control" problem.

From a control standpoint there has been no specific exemption that would permit the withholding of information (on unclassified technology with military application) upon request from any member of the public. "Member of the public" has been interpreted by the Attorney General to mean US citizens or foreign nationals, whether here or abroad. Once the information has been released to a requester, a public disclosure occurs, control is lost, and export may take place without the necessity of an export license.[12] Thus, public release is tantamount to automatic export.

An amendment to the FOIA was advocated that requests for information from the US Government would be limited to US citizens only[13]. While this might preclude direct transfer of technical information to foreign research and development institutions, it would not prevent critical military technology with a "dual-use" from being utilized in a commercial

product "made in USA" and exported (outside the export control laws) to any ally, friend, or adversary. The "Department of Defense Authorization Act of 1984," P.L. 98-94, section 1217 has precipitated a draft DoD Directive 5400.XX, "Release of Technical Data to the Public." The law and this directive provide that technical data with military or space application may be withheld from public disclosure if it is subject to license requirements of the Export Administration Act or the Arms Export Control Act. Release of the data can be made to domestic US contractors with the advice that further dissemination or export may violate the law and will subject them to a fine and/or imprisonment. Militarily critical technology, new distribution statement limitations, and export control will be covered in detail in later sections of this report.

6. Industrial Independent Research and Development

Defense contractors formulate their own independent research and development (IR&D) plan without any Government direction, coercion, or intimidation. The tasks selected by the contractor for an IR&D portfolio are the result of an analysis by the contractor of the market potential and a corporate decision to enter a new or expanding technology field. Government laboratory bench engineers and managers provide an input to industry by evaluating each task on DD Form 1855, "Independent Research and Development Project Technical Evaluation," and providing a numerical score on relevance and accomplishment, and by providing written comments to the contractor. The Government's best input to industry is to provide cogent and clear statements of the service's need. In the Army laboratories, for example, this should be done through the Technical Industrial Liaison Office (TILO). Government engineers review and discuss the IR&D tasks at on-site reviews and by one-on-one technical discussions with the industrial bench engineers, each trying to influence the technical direction of the other but under obligation to protect the proprietary considerations until the technology is productized and marketed. In this technology transfer forum the entire "DoD community," Government and other industry, is eventually aware of the accomplishment.

The defense industry IR&D program is a significant portion of the national defense technology base, since typically it represents 8-10 times the level of DoD program element funding in basic research (6.1) and exploratory development (6.2). Elevation of the US technology

quotient is dependent on effective coordination and transfer of technology between the contractors' IR&D programs and the laboratories. Government engineers are in an ideal position to determine when and where duplication of effort exists between contractors and Government laboratories. In many cases duplication may be warranted if it produces competitive technical approaches to solve the same problem. This situation increases the probability of success. It is also to the advantage of the Government engineer to monitor industry in its application of "dual-use" technology. Many times commercialization of technology is accomplished before militarization.

Industry frequently discloses their innovative and unique ideas in a "United States Patent," a process that puts most of their ideas into the public domain but with economic strings attached. Industry's R&D efforts and concern with classification of national defense information and/or relevance to unclassified militarily critical technology will be discussed in a later section of this report.

C. Domestic Use of Foreign Technical Intelligence

The DoD engineer and his contract industry/academic engineer/scientist obviously need to know about related US defense efforts and IR&D technology tasks in their specific technology field. Another area of great potential value is the knowledge of non-United States military systems and their inherent technologies. Two classes of foreign intelligence beneficial to the DoD research and development community are : (1) the state-of-the-art of relevant foreign technology (referred to as Scientific and Technical Intelligence or (S&TI), and (2) the interaction of US systems with adversary capabilities (referred to as threat studies). Effective use of S&TI (allies and potential adversaries) and threat analyses help the R&D engineer:

- Avoid technological surprise
- Achieve and maintain technological sufficiency
- Select and develop materiel at lowest cost
- Reduce developmental engineering leadtime
- Perceive exploitable vulnerabilities of foreign materiel, leading to effective countermeasure systems.[14]

This intelligence is of the greatest value when it is available in the early stages of project/product development. It must also be updated periodically as additional opportunities in the intelligence collection effort present themselves.

How does the DoD research engineer obtain this information? The DoD intelligence community provides a Foreign Intelligence Office (FIO) at each major Research and Development Center in the Army, Navy, and Air Force. The FIO's are the "user representatives." They speak

the "languages" of the development engineer and the intelligence production community. They anticipate intelligence collection needs and take specific requests. They initiate appropriate requests within the Defense Intelligence Agency (DIA) such as the Air Force Foreign Technology Division, the Naval Intelligence Support Center, and the Army's Foreign Science and Technology Center (FSTC) and Missile Intelligence Agency (MIA). Increased cognizance and effective use of accurate S&TI can bolster the US National Defense effort directly and provide a solid foundation for decisions affecting technology export control.

D. National Security Information Program

It is essential that the public be informed concerning the activities of its Government, but the interests of the United States and its citizens require that certain information concerning the national defense and foreign relations be protected against unauthorized disclosure. A Presidential executive order provides a uniform system for classifying, declassifying, and safeguarding national security information, which if disclosed, could reasonably be expected to cause damage to the national security.

Executive Order 12356 on "National Security Information" became effective on August 1, 1982. This Order revoked Executive Order 12065 of June 28, 1978. Executive Order 12356 prescribes that Information shall be considered for classification if it concerns:

- military plans, weapons, or operations;
- the vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;
- foreign government information;
- intelligence activities (including special activities), or intelligence sources or methods;
- foreign relations or foreign activities of the United States;
- scientific, technological, or economic matters relating to the national security;
- United States Government programs for safeguarding nuclear materials or facilities;
- cryptology;
- a confidential source; or
- other categories of information that are related to the national security and that require protection against unauthorized disclosure as determined by the President or . . . [15]

The executive order further specifies that information determined to concern one or more of the categories prescribed above and the release of which would be harmful to US interests shall be classified at one of the following three levels:

> • "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.
>
> • "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.
>
> • "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.[16]

From a technology transfer point of view there is one exclusion that applies: "Basic scientific research information not clearly related to the national security may not be classified."[17] Before we explore the implication and the concern with unclassified technology with military significance not being adequately "protected," let's review the basics in implementation of the National Security Information program.

The National Security Council provides overall policy direction for the Nation's information security program. The General Services Administration through the Information Security Oversight Office is responsible to implement and monitor the program. Executive Order 12356 is implemented in the DoD by the promulgation of DoD Directive 5200.1, "DoD Information Security Program." That Directive, in turn, authorized the publication of 5200.1-R, "Department of Defense Information Security Program Regulation." As an example of the services' implementation, the

Army issued Army Regulation 380-5, "Department of the Army Information Security Program Regulation," dated 1 September 1983. This regulation is a working level document that provides specific instructions and rules on: definitions, responsibilities, reviews, markings, distribution, dissemination, storage, destruction, classification guidance and industrial considerations, etc. Let's examine security classification guidelines and industrial security operations in more detail.

From an R&D perspective the working level bench engineer and his supervisor are confronted daily with classification decisions on data and analyses. To guide them DoD has directed the preparation and use of Security Classification Guides (SCG's). The SCG's are initiated at the program or project level in the field commands and approved by designated classification authorities, usually at the major subordinate command level.

Department of Defense Handbook DOD 5200.1-14, "Writing Security Classification Guidance," helps the writer systematically determine (1) precisely the specific information elements to be protected, (2) their levels of classification, (3) the duration of classification, and (4) the action to be taken at the end of time in which the classification was effective.

The Handbook suggests that the first consideration in determining what should be classified is to review the "Index of Security Classification Guides," DoD 5200.1-I. Each installation has a security support officer who maintains a copy of the index and can

assist in obtaining the SCG's he does not have on hand. Consistency with existing guides may be a significant factor since there are over 1200 such guides in use.

The next stage is to consider the state-of-the-art in the technology areas of concern and determine what is known and openly published about them, including:

- The known or published status, foreign and domestic;
- The known but unpublished (probably classified) status in the United States;
- The foreign status in friendly and unfriendly countries; and
- The extent of foreign knowledge of the unpublished status in the United States.[18]

Finally in deciding what should be classified or not classified the engineer/project manager should consider the factors that produce directly or indirectly the actual or expected net national advantage. Some of those factors are:

- Fact of interest by the United States Government in the particular effort as a whole or in specific parts that are being considered or emphasized;
- Fact of possession by the United States;
- Capabilities of the resulting product in terms of quality, quantity, and location;
- Performance, including operational performance, as it relates to capabilities;
- Vulnerabilities, countermeasures and counteraction
- Weaknesses, counter-countermeasures;
- Uniqueness, exclusive knowledge by the United States;
- Leadtime, which is related to the state-of-the-art;
- Surprise, which is related to possession and capability to use;
- Specifications, which may be indicative of goals, aims or achievements;
- Manufacturing technology; and
- Associations with other data or activities.[19]

The level of classification criteria is then applied to those characteristics and information determined advantageous for classification. Typically, in a weapons system SCG, performance characteristics and/or specifications are classified confidential, but the details concerning countermeasures and counter-countermeasures are classified secret. The draft SCG is now ready for committee screening at the local level and is forwarded for approval and implementation. The Security Classification Guide is then used by the Government employee as the "reference authority" for classification of technical and management documents prepared on a specific program/project or technology area. How then is the engineer in the defense contractor facility or the contracted scientist in the university research facility required to use the SCG?

A defense contractor, when performing work under a scope of work that may use or produce classified data or analyses is provided a "Contract Security Classification Specification" (DD Form 254). This form is specified for incorporation in the contract by the Defense Acquisition Regulations (DAR) and the form generally cites a specific SCG for the details on what to classify and at what level. The "Industrial Security Regulation" (ISR) and "The Industrial Security Manual (ISM) for Safeguarding Classified Information," DOD 5220.22-M, are prepared and administered by the Defense Investigative Service to insure that the defense contractor adheres to procedures to protect national security information. It prescribes requirements for personnel and facility clearances, receipt, storage and issuance of classified

information, and procedures for obtaining authority to make public release of unclassified information when working on a "classified contract." The ISM does permit a defense contractor to place a "pending classification" on information he has developed and he feels may need protection. He then submits the information to his cognizant IR&D monitor or COTR for a determination.

Do the ISM, AR 380-5, DoD Information Security Program Regulation, and the Executive Order on National Security Information go far enough or go too far in protecting national security?

Only recently has new DoD direction allowed for more restrictive "distribution statements" to:

> protect information and technical data which advance the state-of-the-art or describe new technology in an area of significant or potentially significant military application, or relate to a specific military deficiency of a potential adversary.[20]

This distribution limitation on unclassified militarily critical technology will not impact on transfer of defense technology between Government agencies and their contractors. It should also have a minimal impact on domestic scientific innovation and should not impede the capability of defense industries to compete successfully in national and international markets. Information security instructions do need to reflect the new guidance in distribution limitations on militarily critical technolology and orient the users on the differences.

Two "industrial" loopholes exist in the classified information realm. The laws of the land and the implementing directives do not presently provide for:

- mandatory classification of technical information developed by a contractor on his own, unless he applies for a United States patent; and
- classification of technical information developed by a defense contractor on Government-sponsored IR&D without prior access to classified information unless the Government first acquires a proprietary interest in such product.[21]

In the promotion of domestic technology transfer we have seen how the DoD scientific and technical information program insures transfer of defense technologies within the defense community. We have seen how the Technology Innovation Act and the Freedom of Information Act maximize Federal technology transfer to state and local governments, industry, and individuals. We have also reviewed the process for classifying information to protect it from unauthorized disclosure at home or abroad. Now, let us review the policies for intentional technology export and controls to limit undesirable technology export of both classified and unclassified technical information.

III. TECHNOLOGY EXPORT CONTROL

A. Fundamentals of Export Control

From the bench engineer's perspective, the export control laws and regulations appear rather complex and confusing. Just who is responsible for what and how does that affect me? These are common questions asked by the government laboratory engineer and the defense contractor's engineer. Just as there were several perspectives on domestic technology transfer, the realm of technology export control has two sides and many players.

Intentional technology export is controlled by Federal laws and cabinet level departments and their regulations which define policy and procedures for "controlled" release or retention of technology (and its products) to our Allies, friendly non-aligned nations and sometimes even our "potential adversaries."

Unintentional technology export is hopefully minimized by laws and regulations that establish procedures and guidelines to reduce leakage of innovative technologies that could affect our economic, political, and military well-being.

Generally speaking, classified technology is adequately protected and controls exist to make conscientious decisions to license its sale overseas. Unclassified technology with significant military potential, when it is "dual-use" technology, is sometimes not specifically prevented from export. Many times it is excluded from consideration if it is already in the public domain, and it has in the past been

exempt from export license requirements. Just how do international agreements and US laws on technology export relate to one another, and who does what for whom?

In 1949 the Western Allies formed the Coordinating Committee (CoCom) for multilateral export controls to implement a uniform export control system when dealing with the WARSAW Pact and the Peoples Republic of China (PRC). The CoCom is now comprised of Japan and all the NATO countries except Iceland and Spain. It is a voluntary organization whose decisions can only be implemented through the national policies of its members. These national policies sometimes differ significantly. The CoCom maintains three separate lists covering munitions, atomic energy, and dual-use items. The latter accounts for a majority of the trade matters considered by the group.

The advent of the cold war promoted passage of the Export Administration Act of 1949. Subsequently modified in 1969 and again in 1979, the act provides for controls on export of goods that might assist either the economic or military strength of a potential communist adversary. The responsibility to execute the Export Administration Act (EAA) was placed with the Department of Commerce. The Export Administration Regulation (EAR) provides for stringent Government control in licensing exports. The EAR includes a Commodity Control List (CCL) which (1) identifies the characteristics of the goods and processes of particular concern, (2) the country of destination, and (3) the end-use of the goods. The EAR control also encompasses "technical data." With few exceptions, all exports of

technical data require a general license or a validated license. A general license is analogous to an exemption and a validated license, on the other hand, is a document authorizing a specific export. The EAR process is operated by the Office of Export Administration in the Commerce Department. Most transactions deal with Government agencies other than the Defense Department, but some militarily related transactions require DoD technical input to the decision process.

The Arms Export Control Act of 1976 provides for the Department of State Administration of the "International Traffic in Arms Regulation" (ITAR). The ITAR, first issued in 1954, sets rules for control of the export of military systems, including the "design, production, manufacture, repair, overhaul, processing, engineering, development, operation, maintenance or reconstruction of the implements of war on the US Munitions List" or any technology that advances the state-of-the-art or establishes a new art in any area of significant military applicability."

United States' defense contractors file an application with the Office of Munitions Control in the State Department as the first step to obtain an export license. The Department of Defense is required to establish a "position" on each export license application of military significance or each munitions case. The Department of Defense has promulgated two directives to ensure adequate control of national defense assets and maintain consistency from case-to-case. DoD Directive 5230.11, "Disclosure of Classified Information to Foreign Governments and International Organizations," implements the provisions of the National

Disclosure Policy (NDP-1). It establishes policy, delegates authority, and assigns responsibility for the disclosure and denial of classified military information to foreign governments and international organizations. This directive provides that all US classified military information will be treated as a national security asset, which must be conserved and protected and which may be shared with foreign entities only when there is a clearly defined advantage to the US. The Directive provides that the National Military Information Disclosure Policy Committee (NDPC) is designated as the central authority for the formulation, promulgation, administration, and monitoring of the National Disclosure Policy.[22]

DoD Instruction 5230.17, "Procedures and Standards for Disclosure of Military Information to Foreign Activities," describes the procedures and responsibilities for: (1) disclosure requests and proposals; (2) disclosure decisions; (3) exceptions to the National Disclosure Policy, and (4) expeditious handling of foreign requests. It provides that DoD components participating in activities requiring the disclosure of classified military information shall be informed in writing of: (1) their responsibilities under NDP-1, DoD Directive 5230.11 and this instruction; and (2) the requirements to make certain that the value to the United States is at least equivalent to the value of the information disclosed.

FORDTIS (Foreign Disclosure Technical Information System), a developing computerized data base, was initiated to support the DoD's National Disclosure Policy Committee's decisions. The system's

capability is to be expanded toward maintaining the flow of information required for all technology transfer cases. With FORDTIS, DoD can track cases during the review process, and access historical data and reference files for a variety of case processing, policy formulation, and policy review functions. Expeditious processing and consistency will lead to improved control of national defense technical information.[23]

B. Intentional Technology Export

As strange as it may seem, there are reasons to export one's military technology, both classified and unclassified. First, consider technology transfer to our Allies and friendly non-aligned nations. Transfers through military assistance and foreign military sales of hardware (and its associated technology) allow for improvements in Rationalization, Standardization, and Interoperability (RSI). It obviously produces an Ally with greater military capability and thus creates economic benefit for the US defense contractor. In every transfer situation the United States is required to obtain something at least of equivalent value to the information disclosed and the net result must be clearly an advantage to this nation.

Several general classes of technology transfer vehicles are in place to exchange technology base information with our Allies. Within NATO there is in existence (1) the Advisory Group for Aerospace Research and Development (AGARD), (2) various specific technology panels and working groups, and (3) many memoranda of understanding (MOU's) on technical subjects with individual/collective NATO members. Each of these arrangements are very specific on control of classified information but are less than specific on unclassified information with significant military application.

The United States, the United Kingdom, Canadian, and Australian armies have formed a quadripartite standardization coalition known as the ABCA (American - British - Canadian - Australian) Program. The ABCA countries, including New Zealand working through Australia, establish

efforts to enhance interoperability and maximize resources. Technology exchanges are accomplished through quadripartite working groups and The Technical Cooperation Program (TTCP). The DoD participation is established by DoD Directive 3100.8, "The Technical Cooperation Program." Activities of the TTCP acquaint participating countries with each other's technology base programs to avoid unnecessary duplication and ensure that important gaps in technology will not occur. Obviously these four countries provide for the positive two-way transfer of technology with military application. Protection for classified military information is provided, but there is no provision for controlling unclassified military technology.

Technology transfer mechanisms applicable to <u>any</u> of our allies are MOU's and Data Exchange Agreements (DEA's). Master agreements, known as the Mutual Weapons Development Master Data Exchange Agreement (MWDMDEA) are concluded with specific countries. These agreements provide, on a continuing basis, for the exchange of technical and scientific military information through military channels in areas of mutual technical interest. DoD Directive 2015.4, "Mutual Weapons Development Data Exchange Programs (MWDDEP)," establishes procedures for exchanging certain technical and scientific military information of mutual interest to the United States and other countries through exchange of correspondence, reports, equipment or other material or technical documents, and by visits of technical personnel; and it delineates responsibilities for carrying out the subject program. Bench engineers at the Government laboratories are assigned responsibilities as Technical Project Officers (TPO's). They are the command's technical representative to optimize the value received from the DEA.

A major category of involvement for the Government bench engineer is the technical evaluation concerning approval of various munitions cases. Munitions cases can be in a wide spectrum from a (1) technical assistance agreement, (2) outright foreign military sale (FMS), (3) co-assembly of a military system, (4) co-production of a military system, to (5) co-development of a military system to be used bilaterally or multilaterally. For example, DoD Directive 2000.9, "International Co-production Projects and Agreements Between the United States and Other Countries and International Organizations," prescribes the responsibilities to effect a co-production effort and control the technical data. A definition of "co-production" provides insight to the understanding of this Directive:

> "Co-production" enables an eligible foreign government, to acquire the "know-how" to manufacture, assemble, repair, maintain and operate, in whole or in part, a specific weapon, communication or support system, or an individual military item. The "know-how" may include research, development production data and/or manufacturing machinery or tools, raw or finished material, components or major sub-assemblies, managerial skills, procurement assistance or quality-control procedures.[24]

A co-production effort may be limited or it may extend to a major manufacturing effort requiring the build-up of capital industries. The directive states that classified information and materials will be treated as exchanges between those Governments involved and will be safeguarded by each Government in accordance with existing agreements. In addition to adherence to existing security agreements, a security annex or clause will be developed as a part of the co-production agreement which will cover all security factors involved. The security coverage is sufficiently detailed for classified information when DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International

Organizations," is referenced. With previous distribution statements, control of unclassified technology of military significance was not adequately protected.[25]

Presently DoD Directive 5030.28 (10 March 1970), "Munitions Control Procedures for US Munitions Export License Applications Referred to DoD by the Department of State," delineates procedures for processing munitions export license requests. To reflect consideration of the importance in controlling the disclosure of unclassified technology with military application which may, if exported, constitute a risk to US security interests, a new directive is being staffed. This new directive, 2040.XX (29 December 1982), "Control of International Technology, Goods, Services, and Munitions Transfers," recognizes the deficiency and proposes language that is more definitive. For example, the new directive, when adopted, would limit the transfer of advanced design and manufacturing know-how regarding technology, goods, services, and munitions (items subject to control of the Arms Export Control Act) to those transfers which support specific national security objectives. Further, the new directive would provide that transfers of technology, goods, services, and munitions shall not constitute an unreasonable risk to US security in the degree to which they reduce technological leadtime.[26]

In developing the Army's technical position on a munitions control case, the bench engineer in the Government laboratory answers a series of questions and formulates a technical evaluation. This technical evaluation provides his command official with the information necessary to render a recommendation through channels to the Army staff. An approving

recommendation is stated as "no objection" to export. A disapproving recommendation is stated as "objection" to export for a particular reason. Those questions are:

a. Is the item a standardized US Army item? If the item is in R&D or a commercial type item, explain.

b. Will export of equipment/data require follow-on export of classified equipment/information?

c. Does export of equipment/data impact on current or projected US programs to include R&D, procurement, FMS, Grant Aid, co-development, co-production or data exchange?

d. Is state-of-art related to commodity/data such that export or related plant visit constitutes an unreasonable risk or extraction of US military technology; enable technological lead, or threaten national security?

e. If attached, could drawings/specifications of commodity/data be used for manufacturing purposes?

f. Are RDT&E cost recoverable from this export sale? If so, indicate recoupable cost per unit and describe actions contemplated to recover such costs.

g. Are nonrecurring production costs, recurring support costs, rental charges on GFE or royalty charges recoverable from this export sale? If so, indicate recoupable cost per unit and describe actions contemplated to recover such costs.

h. Is a current end-user request for Price and Availability, Planning and Review, or Letter of Offer and Acceptance for this commodity/data being processed?

i. Does end-user have technical capability to effectively use commodity/data?

j. Is coordination with another agency recommended on this case?

k. What is the maximum security classification of the material or data potentially involved in any use of the requested export?

l. What is the security classification of the requested export?

m. To what other significant military or military-supporting end-use could this item be diverted?

n. Has similar US equipment or related technology been released to foreign countries and/or companies?

o. Is the item presently available in foreign countries? If yes, what is the quantity and quality?

p. For commodity jurisdiction determination cases, what is the recommended munitions list category with rationale?[27]

Now the engineer will also need to consider the existence of unclassified technology that details design and manufacturing know-how.

The concluding topic in these discussions on intentional technology transfer, is the one of occasional export of goods and technology to potential adversaries. These exports are usually related to the environment, space, or health/nutrition, not military systems.

In the early 1970's, bilateral agreements were established with the Soviets to encourage detente. These agreements were "allowed" to expire as a result of the invasion of Afghanistan and the imposition of martial law in Poland.

C. Control of Undesirable Technology Transfer

Leakage of classified and unclassified technology to undesirable recipients can occur through a variety of media. Several control measures have been in effect for many years while some new enforcement activities and control lists are just now becoming fully operational and understood by daily practitioners of military technology development.

Visits by foreign nationals to defense laboratories and US defense contractors are controlled by a DoD visit request authorization. Prior to the visit, information is required of the Government laboratory field location having the technical subject matter expertise. The bench engineer and his supervisor must examine the, usually slim, description of the "purpose of visit" and ascertain the opportunities of discussions based on existing MOU's, DEA's or TTCP exchange agreements with the country in question. These comments are then forwarded through channels to the service level intelligence function for approval. This procedure fairly well controls what classified technical information will be discussed. No specific limitations have existed up until now on unclassified information. The advent and implementation of the new distribution statement limitations should place more stringent controls on unclassified critical military technology know-how.

Technical meetings involving disclosure of classified material are covered by DoD Directive 5200.12, "Security Sponsorship and Procedures for Scientific and Technical Meetings Involving Disclosure of Classified Military Information." The directive precludes a foreign national from attendance in classified meetings unless the head of the DoD component sponsoring the meeting authorizes the attendance in writing and the attendance is consistent with the National Disclosure Policy. No controls have been placed on unclassified information discussed during classified or unclassified sessions. A draft DoD directive, dated 31 August 1983, and titled "Scientific and

Technical Meetings involving Unclassified Technical Data" is presently being coordinated. It will, among other things, place the burden on the local commander to determine potential benefits accruing to the Government versus the possible benefits to potential adversaries by our participation in the meeting. Again, new distribution limitation statements will reduce leakage.

Patents are an established international "protection" for economic reward of the innovative research and development efforts put forth by commercial enterprises. US defense contractors are no exception in wanting future adoption of their ideas to provide economic consideration. All patent applications filed with the Patent and Trademark Office are received and screened for DoD interest. Of the 144,000 patent applications filed each year, about seven-percent are forwarded to DoD agencies for security review.[28] Bench engineers in the defense laboratories are charged with reviewing those applications against system and technology SCG's. Less than one-percent are found to contain classified information. With that finding, and a review by a higher headquarters, the patent office is empowered to block the granting of a patent and to prohibit the inventor from disclosing the invention outside the Government - Defense community. Each year the technical expert in the Government laboratory reviews the patent application for a "stay" in the "secrecy order." In 1979 approximately 3,300 secrecy orders were renewed.[29] This patent review process provides one effective means of controlling inadvertent leaks of classified defense information.

The advent and implementation of militarily critical technology reviews for distribution limitations adds new dimension to the process and may or may not provide for the control of unclassified technology leaks. Enforcement activities to ensure compliance or the conduct of investigations regarding the provisions of the Export Administration Act and the International Traffic in Arms Regulation are conducted by the Commerce Department Office of Export Enforcement, the Federal Bureau of Investigation, and the Treasury Department's Customs Service. Operation EXODUS was initiated by the United States Customs Service in January 1981 to prevent the illegal exportation of strategic technology to the Warsaw Pact nations. EXODUS began with a massive cargo inspection program. This represented a major policy change, as the United States previously mounted only token cargo inspection efforts. Other stages of the project focus on investigations and the active involvement of customs' agents stationed overseas in violation cases.

Exporters and some Members of Congress complain that Operation EXODUS is delaying legal shipments and causing customer problems. The Customs Service's Report on Operation EXODUS acknowledges these complaints, but contends that delays "should diminish substantially in the near future" with the improved training of agents and liaison with the Department of Commerce's licensing staff. Shipment inspection is obviously of limited effectiveness unless all shipments are inspected and then excessive delays would be unsatisfactory and the costs would be prohibitive. Project EXODUS may not stop all illegal or "ignorant of the law" violations but it will instill consciousness and awareness to minimize violations.

The loss of unclassified technology with military application has been the center of concern since it has been the most readily available for a nominal cost and "legal" for acquisition by our Allies and potential adversaries. Information dealing with design and manufacturing know-how for military applicable technologies, but not considered to cause "direct" damage to national security, and therefore be classified, is released for public consumption by the Government laboratories. Additionally, unclassified Government technical documents limited to Government and Government contractors for various reasons were subject to release under Freedom of Information Act requests. Once the subject material was available to the public, it could be purchased by anyone from NTIS and exported without license requirements.

DoD Directive 5200.20, "Distribution Statements on Technical Documents," prescribed two distribution statements for DoD technical documents: Distribution Statement A: "Approved for Public Release; Distribution Unlimited." And Distribution Statement B: "Distribution limited to US Government agencies only; (Reason); Other requests for this document must be referred to (controlling DoD Office)."

Statement "A" could only be used on unclassified documents. Statement "B" could be used on either classified or unclassified technical documents and distribution could be limited for one or more of the four following reasons:

(1) Foreign Information

(2) Proprietary Information

(3) Test and Evaluation

(4) Contractor Performance Evaluation

The previous system made no allowance for limiting unclassified technical information with significant military application.

In October 1983, Secretary of Defense Caspar W. Weinberger issued an "Interim Policy for Marking and Disseminating Defense Technical Documents." The memorandum states:

> "The objective of establishing a system of controls (on technical data) in the Department and defense industry is to protect Defense technology, without incurring substantial cost and minimizing the impact on scientific innovation and the capability of defense industry to compete successfully in domestic and international markets."[30]

It is anticipated the DoD Directive 5200.20, "Distribution Statements on Technical Documents," dated 24 September 1970, will be updated to reflect the new policy statement.

Distribution Statements "A" and "B" remain unchanged but four more "reasons" for limitation are provided as follows:

(5) Export Limitations (License required)

(6) Administrative/Operational Use (precludes automatic distribution of technical manuals, etc.)

(7) Software Documentation (release only in accordance with DoD Instruction 7930.2)

(8) Specific Authority (such as Executive Orders, EAR, ITAR etc.)

A new Distribution Statement "C" provides for the distribution to be limited to US Government agencies and their contractors for reasons (6) and (8) above and as follows:

(9) Critical Technology

To protect information and technical data which advance the state-of-the-art or describe new

technology in an area of significant or potentially significant military application, or relates to a specific military deficiency of a potential adversary. This control on critical technology will allow early dissemination to the US Government and its domestic contractors in a manner that will ensure compliance with the International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR).[31]

Distribution Statement "D" narrows the dissemination to the DoD and DoD contractors for reasons (7), (8), and (9) as above and add the following reason:

(10) Premature Dissemination

(To protect information on system or hardware in the developmental or concept state, which must be protected to prevent premature dissemination.)[32]

Distribution Statement "E" is further limiting to DoD components only. Reasons for limitation are numbers (1), (7), (8), (9), and (10).

Distribution Statement "F" further limits distribution to "only as directed" when the originator determines that information is subject to special dissemination limitations as specified in DoD 5200.1-R, "Major Systems Acquisition."

All statements except "A" may be used on unclassified documents, or on classified documents. This will ensure DoD distribution limitation in additon to need-to-know requirements imposed by DoD 5200.1-R, or in the event the document is declassified.

In addition to Distribution Statements B, C, D, E or F, the following notice is to be affixed to each document so limited:

WARNING

INFORMATION SUBJECT TO EXPORT CONTROL LAWS

This document may contain information subject to the International Traffic in Arms Regulation (ITAR) or the Export Administration

Regulation (EAR) of 1979 which may not be exported, released or disclosed to foreign nationals inside or outside the United States without first obtaining an export license. A violation of the ITAR or EAR may be subject to a penalty of up to 10 years imprisonment and a fine of $100,000 under 22 U.S.C. 2778 or Section 2410 of the Export Administration Act of 1979. Include this notice with any reproduced portion of this document.[33]

This message is clear. The policy is in effect to control unclassified technology with military application. How will the implementation be accomplished?

The implementation of these new distribution statements will begin with the bench engineer in the Government laboratory, in the defense contractor R&D facility, and in the university research facility.

The "subject matter technical expert" must understand that a distribution statement marking is distinct from a security classification marking assigned in accordance with DoD Regulation 5200.1-R, "DoD Information Security Program Regulation" (discussed earlier). A Distribution Statement is used in marking a technical document to denote the conditions and extent of its availability for distribution, release and disclosure without additional authorizations being needed.

Controlling DoD offices are responsible for determining the distribution limitation of each report, whether it is an in-house effort or contract/grant effort or whether the effort is classified or unclassified, based on technology criticality among other things. The Militarily Critical Technologies List (MCTL) is one such reference that can be used in making that determination.[34]

D. The Militarily Critical Technologies List

The Bucy Report of 1976 set forth as its primary conclusion that the control of design and manufacturing know-how is absolutely vital to the maintenance of US technical superiority. This was a shift in emphasis on export controls away from a product or "end item" fixation.

Paralleling the language of the Bucy report, the Export Adminstration Act of 1979 directed the Secretary of Defense to prepare a list of "militarily critical technologies." The Act defined these as technologies which, if exported, would permit a "significant advance" in a military system of any country to which US exports are controlled. The Act stated that this MCTL should emphasize design and manufacturing know-how; keystone manufacturing; inspection and test equipment; and goods accompanied by sophisticated operation, application, or maintenance know-how.

The MCTL is a four volume classified document. Volume 1, the List, is organized into 18 technical area chapters with a total of 460 specific technology subareas. Each of these technologies is analyzed under the following four general categories:

A. Arrays of Know-How (including design and manufacturing know-how) are the know-how and related technical information required to achieve a significant development, production or utilization purpose. Such know-how includes services, processes, procedures, specifications, design data and criteria, and testing techniques.

B. Keystone Equipment (including manufacturing, inspection or test equipment) is the equipment specifically necessary for the effective application of a significant array of technical information and know-how.

C. Keystone Materials are materials specifically necessary for the effective application of a significant array of technical information and know-how.

D. Goods Accompanied by Sophisticated Know-How are goods:

1. the use of which requires the provision (disclosure) of a significant array of technical information and know-how (including operation, application or maintenance know-how), and/or

2. for which embedded know-how is inherently derivable by reverse engineering, or is revealed by use of the goods. [35]

The 18 technology chapters of the MCTL are:

1.0 Computer System and Computer Network Technology
2.0 Computer Hardware Technology
3.0 Computer Software Technology
4.0 Automated Industrial Process Control Technology
5.0 Materials Technology
6.0 Directed Energy Technology
7.0 Semiconductor and Electronic Component Technology
8.0 Instrumentation Technology
9.0 Telecommunications Technology
10.0 Communication, Navigation, Guidance, Control and Identification Technology
11.0 Microwave Technology
12.0 Vehicular Technology
13.0 Optical and Low Energy Laser Technology
14.0 Sensor Technology
15.0 Undersea Systems Technology
16.0 Chemical Technology
17.0 Nuclear- and Energy-Related Technology
18.0 Cryptologic Technology

The remaining three MCTL documents are support volumes which provide reference and background material for the benefit of both the technical and administrative user. The three support documents cover about six chapters each and contain the following types of information:

Military Significance (importance to an adversary of acquiring the technology)

Foreign Capabilities (ability to apply or produce the technology)

Representative Applications (provides sample of military or dual-use products and processes)

Transfer Mechanisms (discusses production, licensing, service arrangements, marketing)

Technical Notes (detailed descriptions of the technology)

Goods Which Employ the Technology and Have Intrinsic Military Value (correlation between technologies and end products contained in the Commodity Control List and Munitions List)

Additional Reference Materials (bibliography of all the reference materials used)

The Defense Department has produced the MCTL by involving technical specialists from DoD, the military services, service laboratories, other government agencies, and industry. Approximately 80 industrial firms formally reviewed the MCTL. The MCTL is updated annually; the fourth edition was distributed in October 1983.

The criteria for selection of "candidate technologies" for the MCTL included:

- Technology which is not already possessed by potential adversary, nor is it readily available.
- Technology which provides advantage to US in terms of performance, reliability, maintenance and cost over systems currently employed by adversary.
- Technology which is on CIA's projection of Soviet acquisition targets.
- Technology which is related to emerging technology with high potential for having an impact for advanced military application.

The MCTL has come under criticism from license reviewers, industry, and academia for a variety of reasons. Some contend that the MCTL contains too many items and that the individual technology subjects are too broad and not specific as to exactly what technical information is critical. The question of "dual-use" technologies and the availability of the information already being used in the commercial sector diminishes the reason for flagging the technology to preclude export and additional public release. It is a well known fact that commercialization of a technology can be accomplished before militarization. In utilizing the MCTL, a license case reviewer or engineer may find a lack of information covering his specific area of interest. He may also find technology discussions that need modifying or even eliminating. The panel on Scientific Communications and National Security identifies the following reasons for removing a technology from the MCTL to concentrate only on items that are "truly critical":

- Science and technology whose transfer would not lead to a significant near-term improvement in Soviet defense capability;
- Science underlying a mature technology--that is, a technology that is evolving slowly;
- Science underlying dual-use technology that is not process-oriented;
- Components used in militarily sensitive devices that in themselves are not sensitive.[37]

Even though a great deal of work has gone into preparing the present MCTL, it can always use refinement, additions, and deletions. The inputs must come from the bench engineer, since he is the subject

matter expert. The bench engineer is supposed to be knowledgeable of the estimates produced by the intelligence community, know what is being developed by the Allies, and what is being accomplished in commercial industry as well as by the defense community. Through the weekly use of his portion (10 pages) of the MCTL in preparing distribution statements and reviewing munitions control cases, the MCTL will "mature."

The length of the MCTL and the feeling that "we can't adequately control everything well" leads to the idea of prioritization. Some of the listed critical technology items should be removed. Those decisions should be made by the DoD technical staff-specialist who has the broad across-the-board purview of a particular group of technology areas.

The control of technology with significant military application has been significantly enhanced by the promulgation of the Secretary of Defense's policy on distribution limitations. But what about the consternation of the bench engineer and his supervisor when they are using the SCG and the MCTL to determine what information is classified, what information is unclassified -- critical technology, and what information is unclassified and suitable for "public release - distribution unlimited." An even more difficult job may be the preparation of the SCG's and submission of inputs on MCTL specific technologies. Where do you draw the lines between classified, unclassified militarily critical technology, and unclassified information?

Some general rules and common sense may be the most appropriate method. Considering only research, development and acquisition technical and program information, the following rules may be applied:

Rule 1: Consider Classifying This Information - Information relating to (1) performance and capabilities, (2) specifications, (3) vulnerabilities, (4) procurement and production plans and schedules, and (5) operations. The level of classiification is based on the "advantage factors" discussed earlier from AR 380-5, "Department of the Army Information Security Program Regulation," in its Appendix E.

Rule 2: Consider Denoting This Information as Militarily Critical Technology - Information that specifically provides the "know-how" to design, fabricate, process, assemble, manufacture, and test military hardware and software.

Rule 3: Consider Maintaining This Information Unclassified and Applicable to "Public Release -- Distribution Unlimited" - Basic scientific and technical information developed in the Government laboratory, in the defense industry's R&D center, on IR&D, on contract, in the non-defense industry's engineering and manufacturing facility, and in the university research facility -- until the "state of emergence" is evident. (The transition from basic research (6.1) to exploratory development (6.2) with specific military application as denoted in Rule 2 above.)

The bench engineer and his supervisor must keep in mind that their use of the MCTL in munitions case reviews and in establishing

distribution statement limitations must be totally from a technical standpoint with the full knowledge in the state-of-the-art status of the adversaries, the Allies, the US Defense community and US domestic industry. Their technical recommendations on technology transfer cases will be considered at a higher level along with the political, military and economic considerations. Those controls are established outside the militarily critical technologies areas.

IV. SUMMARY

A. The Roles of the Bench Engineer

The bench engineers in the Government laboratories, in the defense industries, and in the university research facilities are the catalysts to propagate technology within the defense community and the US domestic scientific and technical arena while ensuring that defense information and critical military technology is appropriately controlled. It is the "working level" people "working together" that will be able to optimize the situation over the conflict between the two sides of the technology transfer question. What "do's" and "don'ts" are applicable to these bench engineers in this situation?

The bench engineer should do the following:

1. Become a "subject matter expert" on technology status in the US defense community, commercial industry, academia, and the international arena (Allied and adversarial).

2. Make technology transfer considerations, both domestic and export control, a subject at all technical meetings, conferences, and workshops.

3. Ask the information security specialist for assistance on preparing Security Classification Guides. Use Security Classification Guides.

4. Make use of the local supporting technical library.

5. Ensure that technical information is provided to the appropriate Information Analysis Center (IAC), and DTIC. Utilize DTIC and the IAC's that support the area of interest.

6. Participate in IR&D projects as a defense contractor's principal investigator or a Government lab's evaluator.

7. Keep in mind the transfer of Government developed technology with potential application to state/local governments, commercial industry and individuals. Coordinate submissions with Office of Research and Technology Application (ORTA) representative to the Federal Laboratory Consortium (FLC) and The Center for Utilization of Federal Technology (CUFT).

8. Use local Foreign Intelligence Office (FIO) support function to obtain scientific and technical intelligence on Allied and adversary military equipment.

9. Participate in technical professional societies (local, national, or international) as a chapter officer, presenter, or conference attendee.

10. Participate in service support organizations such as the Association of the United States Army (AUSA) and the Air Force Association (AFA).

11. Utilize the MCTL for export case reviews and distribution statement limitation determinations. Provide technical input to DoD to update MCTL data as the situation changes.

12. Obtain Public Affairs Office clearance on all information/ documentation to be placed in the public domain.

The Don'ts for the bench engineer in the defense community are:

1. Don't disseminate technical information without proper consideration of security or military criticality.

2. Don't restrict distribution of technical information just because it takes an extra effort to obtain approval for public release.

3. Don't allow technical discussions and presentations to contain material (classified or unclassified militarily critical technology) beyond the scope approved for the audience.

4. Don't become upset over individual munition case and export license final decisions when they appear to be contrary to the technical position. Economic, political, and military considerations also contribute to overall national security and prosperity.

5. Don't overlook any defense technology area for possibilities of transfer to domestic industrial applications.

6. Don't discount the benefits that can be obtained by joint, cooperative technology exchange agreements among US Allies.

7. Don't become complacent -- effective domestic technology transfer and adequate assesments on technology status take a concerned and informed engineer.

B. National Security by Accomplishment

The National Academy of Science panel on Scientific Communications and National Security sets forth the postulate that "Security by Accomplishments" is better than "Security through Secrecy," and that it represents a national strategy for long-term security through economic, technical, scientific and intellectual vitality.[38]

> A strategy of security by accomplishment has several institutional components. First, universities have the tasks of training new scientists and engineers and conducting basic research, the source of long-term progress. Second, government laboratories undertake research directed to particular national interests in defense, medicine, space, energy, and agriculture. Third, industry translates the results of research into new commercial and defense technology. It is important that all these institutions attain their full potential, for economic as well as for military reasons. Open scientific communication plays an important part in keeping scientists and engineers in Government, industry, and universities aware of each others' needs and findings.[39]

Domestic technology transfer is enhanced in an open society. In the long run, the technological lead of the US is maintained through effective vigorous research and development and a conscious effort to prevent the undesirable export of critical military technologies. The participation of the defense community bench engineer and his supervisor is the key to moderation and balance in the technology transfer controversy. That moderation and balance will contribute to the achievement of the desired technological leadtime.

REFERENCES

1. Inman, Bobby R., Admiral, Statement of Deputy Director of Central Intelligence before the Subcommittee on Science, Research and Technology and Subcommittee on Investigations and Oversight of the Committee on Science and Technology, US House of Representatives, 29 March 1982, and before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, U.S. Senate, 11 May 1983, p. 10.

2. US Department of Defense, Office of the Director of Defense Research and Engineering, An Analysis of Export Control of US Technology - A DOD Perspective, known as the "Bucy Report", 4 February 1976, pp. 4, 5.

3. National Academy of Sciences, Scientific Communications and National Security, 30 September 1982, p. 15.

4. Inman, pp. 13-15.

5. National Academy of Sciences, p. 22.

6. Ibid.

7. Ibid, p. 24.

8. Department of Defense, Defense Technical Information Center, Information Analysis Centers - Profiles for Specialized Technical Information, known as the "Red Book," April 1981 and updated January 1983, pp. 6-25.

9. Ibid, pp. 2, 3.

10. US Department of Commerce, Federal Technology Catalog, January 1983, p. i.

11. US Department of Defense, Control of Unclassified Technology with Military Application, Advanced Technology, Inc., Final Report, 15 April 1983, p. A-28. (Hereafter refered to as "Applied Technology, Inc., Final Report")

12. Ibid, p. 20.

13. Ibid.

14. US Army Materiel Development and Readiness Command, RDTE Managers Intelligence and Threat Support Guide, 17 June 1983, p. I-2.

15. National Academy of Sciences, p. 149.

16. Ibid, p. 145.

17. Ibid, p. 153.

18. US Department of the Army, Army Regulation 380-5, p. E-15. (Hereafter referred to as "AR 380-5").

19. Ibid, p. E-16.

20. Weinberger, Caspar W., Memorandum for Secretaries of Military Departments, et al, Control of Unclassified Technology with Military Application, 18 October 1983, p. 8. (Hereafter referred to as "Weinberger Memorandum").

21. AR 380-5, paragraph 2-702, p. II-8.

22. Applied Technology, Inc., Final Report, p. A-24.

23. Weinberger, Caspar W., The Technology Transfer Control Program, report to the 98th Congress, February 1983, pp. 14, 17, 18.

24. Applied technology Inc., Final Report, p. A-5.

25. Ibid, p. A-6.

26. Ibid, p. A-12.

27. US Department of the Army, Army Regulation 12-6, DA Form 4605.

28. Applied Technology, Inc., Final Report, p. 31.

29. National Academy of Sciences, p. 100.

30. Weinberger Memorandum, p. cover.

31. Ibid, p. 8.

32. Ibid.

33. Ibid, p. 9.

34. Ibid, p. 2.

35. US Department of Defense, Coordination Draft Militarily Critical Technologies List (U), 17 August 1983, p. 5.

36. Ibid, p. v.

37. National Academy of Sciences, p. 65.

38. Ibid, p. 45.

39. Ibid.

SELECTED BIBLIOGRAPHY

1. "ABCA TEAL", Army RD&A, Vol 23, No. 1, January-February 1982.

2. Coleman, Herbert J. New Rules Altering Joint Efforts, Aviation Week and Space Technology, 30 May 1983, p. 78-81.

3. Freedenberg, Paul, U.S. Export Controls: Issues for High Technology Industries, National Journal, 18 December 1982, p. 2190-2193.

4. "How Russia Steals U.S Defense Secrets", U.S. New & World Report, 25 May 1981, p. 39-41.

5. Inman, Bobby R. Admiral, Statement of Deputy Director of Central Intelligence before the Subcommittee on Science, Research and Technology and Subcommittee on Investigations and Oversight of the Committee on Science and Technology, US House of Representatives, 29 March 1982 and before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, US Senate, 11 May 1982, Washington: Government Printing Office, 1982.

6. Levi, Bob, Eighth Annual Meeting and International Symposium, Technology Transfer Society Meeting Announcement, 20-22 June 1983.

7. Madison, Christopher, Congress, Administration Split on How to Plug Technology Leaks to Soviets, National Journal, 19 February 1983, p. 380-383.

8. Madison, Christopher, Trading with the Soviets - Should We Offer a Carrot or Wield a Stick?, National Journal, 9 May 1981, p. 820-8233.

9. National Academy of Sciences, Scientific Communications and National Security, Washington: 30 September 1982.

   (excellent overall perspective and advocate position for open scientific communications)

10. Ropelewski, Robert R. Study Urges Strong Government Policy in International Cooperation, Aviation Week and Space Technology, 30 May 1983, p. 287-290.

11. Technology Transfer: A Policy Nightmare, Business Week, 4 April 1983, p. 94-100.

12. Update of U.S. Export Controls Urged, Aviation Week and Space Technology, 11 June 1979, p. 119-121.

13. US Army Materiel Development and Readiness Command, RDTE Managers Intelligence and Threat Support Guide, Alexandria, Va., 17 June 1983.

14. US Department of the Army, Army Regulation 380-5, Department of the Army Information Security Program Regulation, Washington: 1 August 1983.

15. US Department of the Army, Army Regulation 12-6, Munitions Control Program, Washington: 15 May 1980.

16. US Department of Commerce, Federal Technology Catalog, NTIS Tech Notes Annual Index, Springfield, Va., January 1983.

17. US Congress, Office of Technology Assessment, Technology and East-West Trade: An Update, Library of Congress Catalog Card Number 79-600203, Washington: Government Printing Office, 1983.

18. US Laws, Statutes, etc. Public Law 480, 96th Cong. 21 October 1980. "Stevenson-Wydler Technology Innovation Act of 1980."

19. US Laws, Statutes, etc. Public Law 94, 98th Cong. November 1983. "Department of Defense Authorization Act, 1984" Section 1217, authority to withhold from public disclosure certain technical data.

20. US Department of Defense, Office of the Director of Defense Research and Engineering, An Analysis of Export Control of US Technology - A DOD Perspective, known as the Bucy Report, Washington, 4 February 1976.

    (A Report of the Defense Science Board Task Force on Export of US Technology, established perspective to focus on technology and not end products of tehnology)

21. US Department of Defense, Soviet Military Power, Second Edition, March 1983, Washington: Government Printing Office 1983.

22. US Department of Defense, Defense Technical Information Center, Information Analyses Centers - Profiles for Specialized Technical Information, known as the "Red Book," Alexandria, Va., April 81, updated January 1983.

23. US Department of Defense, Coordination Draft - Department of Defense Directive - Militarily Critical Technology, Number 2040.1-L, Washington, undated.

24. US Department of Defense, Office of the Secretary of Defense, Index of Security Classification Guides, Washington, January 1983.

25. US Department of Defense, DoD Scientific and Technical Information Program, DoD Directive Number 3200.12, Washington: 15 February 1983.

26. US Department of Defense, Control of International Technology, Goods,Services, and Munitions Transfers, Draft DoD Directive Number 2040.XX, Washington: 29 December 1982.

27. US Department of Defense, Release of Technical Data to the Public, Draft DoD Directive Number 5400.XX, Washington: 21 November 1983.

28. US Department of Defense, Scientific and Technical Meetings Involving Unclassified Technical Data, Draft DoD Directive Number. XXXX.XX, Washington: 31 August 1983.

29. US Department of Defense, Control of Unclassified Technology with Military Application, Office Deputy Under Secretary of Defense for Policy Contract MDA903-83-C-0055, Advanced Technology System, Inc., Final Report, Vienna, Va., 15 April 1983.

30. US Defense Investigative Service, Security Awareness Bulletin, No. 2-83, Richmond, Va., Feb 1983.

31. Weinberger, Caspar W., US Department of Defense, Memorandum for Secretaries of Military Departments, et al, Control of Unclassified Technology with Military Application, 18 October 1983.

32. Weinberger, Caspar W., The Technology Transfer Control Program, Report to the 98th Congress, February 1983, Washington: US Department of Defense, February 1983.

THE TACTICAL WEAPON GUIDANCE AND CONTROL INFORMATION ANALYSIS CENTER (GACIAC)

GACIAC is a DoD Information Analysis Center operated by IIT Research Institute under the technical sponsorship of the Joint Service Guidance and Control Committee with members from OUSDRE, Army, Navy, Air Force, and DARPA. The U.S. Army Missile Command provides the Contracting Officer's Technical Representative. Its mission is to assist the tactical weapon guidance and control community by encouraging and facilitating the exchange and dissemination of technical data and information for the purpose of effecting coordination of research, exploratory development, and advanced technology demonstrations. To accomplish this, GACIAC's functions are to:

1. *Develop a machine-readable bibliographic data base- currently containing over 30,000 entries;*
2. *Collect, review, and store pertinent documents in its field of interest- -the library contains over 9,000 reports;*
3. *Analyze, appraise and summarize information and data on selected subjects;*
4. *Disseminate information through the GACIAC Bulletin, bibliographies, state-of-the-art summaries, technology assessments, handbooks, special reports, and conferences;*
5. *Respond to technical inquiries related to tactical weapon guidance and control; and*
6. *Provide technical and administrative support to the Joint Service Guidance and Control Committee (JSGCC).*

The products and services of GACIAC are available to qualified industrial users through a subscription plan or individual sales. Government personnel are eligible for products and services under block funding provided by the Army, Navy, Air Force and DARPA. A written request on government stationery is required to receive all the products as a government subscriber.

Further information regarding GACIAC services, products, participation plan, or additional copies of this Special Report may be obtained by writing or calling: GACIAC, IIT Research Institute, 10 West 35th Street, Chicago, Illinois 60616, Area Code 312, 567-4519 or 567-4544.